Single channel RF or IR + coding

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 271 887 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.01.2003 Bulletin 2003/01

(51) Int Cl.[7]: **H04L 29/06**, G07F 7/10

(21) Application number: **02013660.2**

(22) Date of filing: **20.06.2002**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.06.2001 US 896636**

(71) Applicant: **Nokia Corporation**
02150 Espoo (FI)

(72) Inventor: **Ikonen, Ari**
21280 Raisio (SE)

(74) Representative: **Lindberg, Klas Valter Bo et al**
Awapatent AB
P.O. Box 11394
404 28 Göteborg (SE)

(54) A system and method for transmitting data via a wireless connection in a secure manner

(57) A system and method for enabling a user of a remote controller to transmit a PIN over a wireless connection in a secure manner. In accordance with the present invention, a terminal device, used for conducting transactions with a service provider, is coupled to the service provider via a data network and a display such as that of a television or personal computer. The same remote control device (either IR or RF) that is used to operate the display is also used to transmit an encoded PIN to the terminal. Session-specific coding rules for encoding the PIN are displayed to the user to guide him through the encoding process. Upon receipt of the encoded PIN, the terminal decodes it, validates it and, if appropriate, permits access to the requested transaction or service.

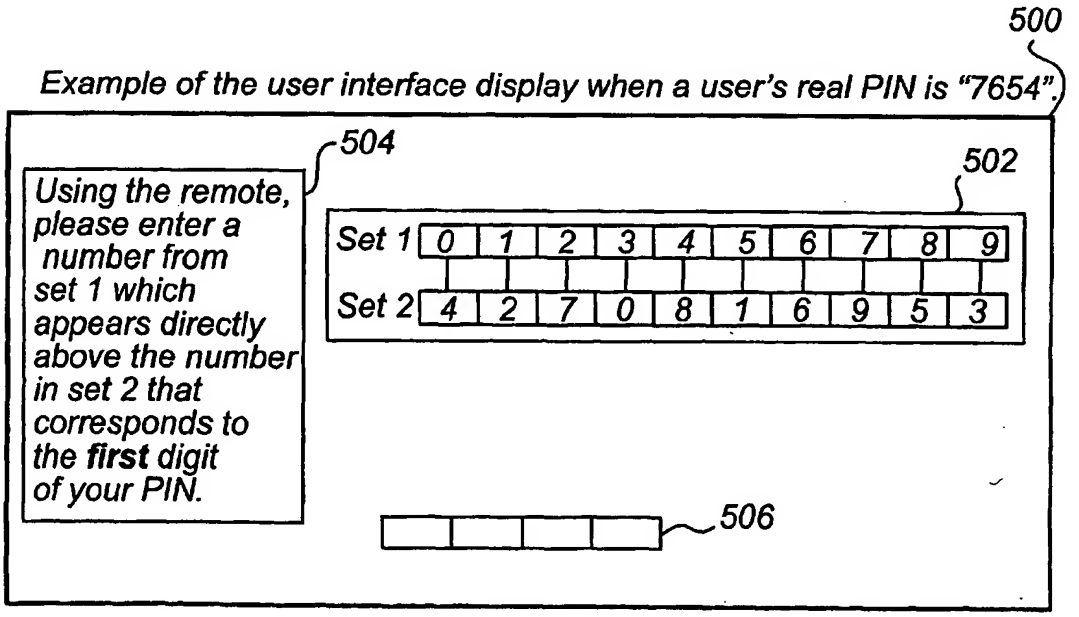

Fig. 5A

EP 1 271 887 A1

Description

FIELD OF THE INVENTION

[0001] This invention relates generally to wireless communications, and more particularly, to a system and method for enabling a user of a remote control device to transmit sensitive data over a wireless connection in a secure manner.

BACKGROUND OF THE INVENTION

[0002] The use of infra-red and radio frequency remote controllers to control electronic equipment such as televisions, set-top boxes (cable or satellite), personal computers, garage door openers, automobile locks and the like is well known. One drawback to the use of such controllers is the ease in which their signals can be intercepted by unscrupulous individuals with what is termed an "electronic grabber" for unauthorized use at a later time. Thus, to the extent that sensitive data is transmitted using such remote controllers, absent safeguards, the transmission is anything but secure.

[0003] A known way of avoiding interception of such signals is to position the controller and the equipment close to one another and transfer sensitive data, at a power level lower than that normally used for transmitting other types of information. Since the power used to transmit the sensitive data is very low, it is difficult for a "grabber" to detect the data. However, having to place the remote controller and the equipment in close proximity of one another to avoid interception goes a long way toward eliminating the convenience associated with using a remote controller.

[0004] Another known way to prevent the interception of signals is for the remote controller to encode sensitive data with a code that is changed automatically in both the controller and the equipment. In this manner, an unauthorized user who is able to detect the transmitted signal is unable to access the equipment by reusing the same signal format. However, this technique requires the use of a specialized remote controller capable of performing the encoding process.

SUMMARY OF THE INVENTION

[0005] The above-identified problems are solved and a technical advance is achieved in the art by providing a system and method for enabling a user to enter data over a wireless connection in a secure manner.

[0006] An exemplary method includes displaying rules for encoding data, receiving encoded data over a wireless connection and decoding the encoded data.

[0007] In another embodiment, an exemplary method includes viewing rules for encoding data, encoding the data in accordance with the rules and transmitting the encoded data over a wireless connection.

[0008] In an alternate embodiment, an exemplary method includes displaying rules for encoding a PIN, receiving an encoded PIN over a wireless connection from a remote controller, decoding the encoded PIN, validating the PIN and if the PIN is valid, authorizing an activity.

[0009] In yet another embodiment, an exemplary method includes viewing rules for encoding a PIN, encoding the PIN in accordance with the rules, transmitting the encoded PIN over a wireless connection and if said PIN is valid, engaging in an activity.

[0010] In still another embodiment, an exemplary method includes transmitting, for display, rules for using the wireless device to encode data transmitted over the wireless connection; receiving data encoded in accordance with the rules; and decoding the encoded data.

[0011] Thus, in accordance with the present invention, a user of a conventional remote control device is provided with a convenient mechanism for transmitting sensitive data over a wireless connection in a secure manner.

[0012] Other and further aspects of the present invention will become apparent during the course of the following description and by reference to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a block diagram of an overview of an exemplary system for enabling a user of a remote control device to conduct secure transactions.

[0014] FIG.2 is a block diagram of an exemplary terminal device.

[0015] FIG. 3 is a flowchart illustrating an exemplary process by which the terminal device of FIG. 3 enables secure entry of a PIN.

[0016] FIGS. 4A-4C illustrate exemplary coding records generated during the process of FIG. 3.

[0017] FIGS. 5A-5E illustrate exemplary screens displayed to the user during the process of FIG. 3.

DETAILED DESCRIPTION

[0018] Referring now to FIG. 1, there is shown, in accordance with one embodiment of the present invention, a system 100 for enabling a user of a remote control device to conduct secure transactions.

[0019] As shown in FIG. 1, system 100 includes an electronic device 110, a remote controller 120 and a terminal device 200. The electronic device 110 may be a television with a set-top box, a personal computer, etc., or any device with a display 112, such as a cathode ray tube. Device 110 also includes an infrared receiver 114 for receiving conventional control commands from remote controller 120.

[0020] As further shown in FIG. 1, remote controller 120 includes a numeric key pad 122, function keys 124, infrared transmitter 126 and/or radio frequency transmitter 128. Transmitter 128 may be, for example, a low power radio frequency ("LPRF") transmitter such as a

Bluetooth transmitter. In one embodiment, remote controller 120 uses infrared transmitter 126 to transmit conventional control commands (e.g., On, Off, Channel Up, Volume Down, etc.) to electronic device 110. A user employs numeric keypad 122 and function keys 124 to enter the control commands in a conventional manner.

[0021] Terminal device 200 of FIG. 1 includes a smart card-based application by which a user of remote controller 120 can conduct secure transactions with service provider 140. The smart card-based application may require the user to transmit a personal identification number ("PIN"), payment information and/or other sensitive data to terminal 200 for a variety of reasons including, but not limited to, ensuring that the transaction is authorized. The user transmits such data to terminal device 200 using either infrared transmitter 126 or radio frequency transmitter 128 of remote controller 120, depending upon the type of receiver employed by terminal 200 for this purpose. (As also shown in FIG. 1, terminal device 200 includes infrared and/or radio frequency receivers (220, 222) for receiving such information from controller 120.) The user employs numeric keypad 122 and function keys 124 to transmit sensitive data to terminal 200. Moreover, one of the function keys 124 can be predefined to permit switching transmissions between electronic device 110 and terminal 200.

[0022] In accordance with the present invention, terminal 200 advantageously guides the user through the process of encoding sensitive data, prior to transmission to terminal 200, thereby ensuring that the transmission of such data is secure. Guidance is provided in the form of instructions and/or other information displayed to the user on display 112 of electronic device 110, as will be discussed in detail hereinafter in connection with FIG. 3. Thus, in accordance with the present invention, sensitive data can be transmitted in a secure manner from a standard remote controller 120, which otherwise does not have a mechanism for encoding data.

[0023] Once terminal 200 has decoded and validated the received PIN, the user is permitted to carry on the requested transaction with service provider 140. This may require the user to select from various application-specific options from display 112 relating to the transaction using remote controller 120. Such transactions may include purchasing goods or services over the Internet, purchasing a "Pay-Per-View" movie from a cable television operator, conducting electronic banking and the like, which typically involve transmitting payment information, such as a credit card number, to service provider 140. To this end, terminal device 200 is coupled to service provider 140 via a data connection 150 such as a cable television connection, an Internet connection, a wireless connection, or the like.

[0024] FIG. 2 is a block diagram of an exemplary terminal device 200. In one embodiment, terminal device 200 includes a CPU 205 together with associated memory (210, 215) for enabling a PIN and/or or other information necessary for conducting a secure transaction, to be transmitted by remote controller 200 over a wireless connection in a secure manner, as will be discussed in detail hereinafter in connection with FIG. 3.

[0025] As shown in FIG. 2, CPU 205 is also coupled to graphics chip 230 for interfacing with display 112 of electronic device 110 to display instructions to the user for use in encoding data, such as a PIN, for transmission to terminal 200. The displayed instructions are derived, in part, from data that CPU 205 receives from random number generator 235, as also will be discussed in detail hereinafter in connection with FIG. 3. CPU 205 is also coupled to an infrared or radio frequency receiver (220, 222) for receiving the encoded PIN and subsequent commands from remote controller 120. The user's PIN is pre-stored in smart card 225 of user terminal 200. It will be understood that smart card 225, being a detachable device, allows various users, each with their own smart card 225 having their own PIN pre-stored therein, to transmit information over a wireless connection in a secure manner via a "public" terminal 200, provided that the terminal also includes a mechanism for communicating with service provider 140. CPU 205 decodes the encoded PIN in accordance with the decoding rules stored in memory (210, 215). CPU 205 then validates the decoded PIN by comparing it with the PIN received from smart card 225. If the decoded PIN is a valid PIN, the user is provided access to service provider 140 via communications port 240.

[0026] In an alternate and perhaps even more secure embodiment, the hardware and software necessary for conducting secure transactions resides entirely within smart card 225 or other secure detachable device. In this alternate embodiment, the random number generator 230 resides in card 225 and both the receivers (220, 222) and graphics chip 230 are connected directly to card 225. In other words, all receiving, decoding and validating of PINs are performed by smart card 225 (i.e., the smart card's CPU and associated memory). In this way, information relating to the PIN is not shared with main CPU 205. Thus, in this embodiment, CPU 205 and associated memory (210, 215) are used only for conducting the requested transaction after it has been authorized by smart card 225.

[0027] In a yet another embodiment, all of the hardware and software necessary for conducting secure transactions in accordance with the present invention resides at service provide 140, rather than within terminal 200. Thus, in this embodiment, service provider 140 generates instructions and/or other information necessary to visually guide the user through the process of encoding the PIN. In this regard, service provider 140 transmits this information via data connection 150 to the terminal device 200 for presentation to the user on display 112. Also, all remote controller 120 commands needed for conducting secure transactions (e.g., encoded digits of a PIN) are transmitted to service provider 140 via terminal device 200. Thus, in this embodiment, decoding and validating of PINs is performed at service

provider 140, rather than at terminal 200.

[0028] FIG. 3 is a flowchart illustrating an exemplary process by which terminal 200 enables a user of a remote control device to conduct secure transactions. In step 305 of FIG. 3, terminal 200 receives a request for a transaction from a user of remote controller 120. The user may transmit the request to terminal 200 over the infrared or RF connections, e.g., by depressing a function key 124 of controller 120 that has been pre-defined for this purpose. In step 310, terminal 200 determines the length of the PIN needed to conduct the requested transaction; more secure transactions may require entry of a longer PIN. It is to be understood that the data that can be transmitted in accordance with the present invention is not limited to PINS, but rather, can include any data sought to be transmitted in a secure manner over a wireless connection. Such data includes, but is not limited to, user account information or credit card numbers used to pay for goods or services that are the subject of the requested transaction.

[0029] Steps 315-330 of FIG. 3 relate to an exemplary method for generating the encoding rules that will be displayed to the user to guide him through the process of encoding his PIN for secure transmission. These rules will also be stored by terminal 200 for decoding the encoded PIN received from the user. FIGS. 4A-C illustrate exemplary coding records generated during steps 315-330; thus, each of these figures is referenced below in connection with the discussion of these steps.

[0030] In step 315, terminal 200 generates and stores a first set of numbers 0-9. The first set of numbers is shown in FIG. 4A. In step 320, terminal 200 generates and stores a second set of numbers 0-9, wherein the numbers of the second set are placed in random order, as shown in FIG. 4B. The second set of numbers is generated using random number generator 230 in a manner well-known in the art. In step 325 of FIG. 3, terminal 200 associates each number in the first set with a number in the second set, as illustrated by the vertical lines in FIG. 4C. In step 330, terminal 200 stores this association for purposes of both displaying it to the user to guide him through the encoding process and thereafter using it to decode an encoded PIN received from the user.

[0031] It is to be understood that the above-described association is intended to be illustrative rather than limiting. For example, the first set of numbers, rather than, or in addition to, the second set of numbers, could also be randomly generated. Also, the association may include characters such as letters of the alphabet or symbols (e.g., %, &, etc.) rather than, or in addition to, numerals, provided that the remote controller 120 includes keys for transmitting such letters or symbols as the need arises.

[0032] In step 335, terminal 200 displays the association of FIG. 4C to the user. In step 340, the user is prompted to transmit a number from the first set of numbers that is associated with the number in the second set that corresponds to the first digit of the user's previously assigned or selected PIN. In step 345, terminal 400 receives the first encoded digit of the user's PIN. In step 350, terminal 200 prompts the user to transmit a number from the first set that is associated with the number in the second set that corresponds to the next digit of the user's PIN. In step 355, the next encoded digit of the PIN is received. In step 360, terminal 200 determines whether the digit received in step 350 was the last digit of the user's PIN. If the digit received was not the last digit, then steps 350 and 355 are repeated. If the digit received was the last digit, then, in step 365, terminal 200 decodes the encoded PIN by comparing each digit of the encoded PIN with the stored association.

[0033] In step 370, terminal 200 then determines whether the decoded PIN is a valid PIN. If the decoded PIN is a valid PIN, in step 375, terminal 200 provides the user with access to the requested transaction. If, however, it is determined in step 370 that the decoded PIN is not valid, then the process set forth in steps 315 through 370 is repeated in attempting to obtain a valid PIN from the user. Recall that steps 315-330 relate to generating the encoding rules displayed to the user. These rules are preferably changed whenever a re-attempt is made at obtaining a valid PIN or each time there is a new request for a transaction, as an added measure of security.

[0034] FIGS. 5A-5E illustrate an exemplary user interface displayed during the process of FIG. 3. For purposes of illustration, it is assumed that the user's PIN is "7654". FIG. 5A illustrates the first screen displayed to the user (i.e., before the user has transmitted any digits of an encoded PIN to terminal 200). As shown in FIG. 5A, the screen displayed to the user includes the association 502 between the first set of numbers and the second set of numbers generated by terminal 200, as discussed above in connection with FIG. 3. The screen also includes instructions 504 for using the displayed association to encode the first digit of the user's PIN. In particular, the instructions request the user to use remote controller 120 to enter a number from set 1 which appears directly above the number in set 2 that corresponds to the first digit of the user's PIN. The displayed association 502 together with the instructions 504 for using them are one example of rules for encoding a user's PIN. The user, knowing that his PIN is "7654", and viewing the on-screen association 502 between the first and second sets of numbers, will select the number "2". This is because the number "2" in the first set appears directly above the number "7" in the second set, which, in turn, corresponds to the first digit of his PIN. The user will then use remote controller 120 to transmit the number "2" to terminal 200 as the first digit of his encoded PIN. Screen 500 also includes fields 506 for providing the user with visual feedback that the transmitted digits have been received by terminal 200, as will become apparent in connection with the discussion of FIGS. 5B-5E.

[0035] FIG. 5B illustrates the second screen dis-

played to the user. As shown in FIG. 5B, the second screen contains substantially the same information as the first screen, except that an asterisk appears in field 506a to provide the user with visual feedback that the first digit has been received. It will be understood that the use of an asterisk in this manner is intended to be illustrative, rather than limiting, and that any mechanism for providing visual feedback may be employed. The only other difference between the first and second screens is that the second screen's instructions are directed to requesting entry of the second digit of the user's PIN, rather than the first digit, in accordance with the displayed association. Once again, since the user's PIN is "7654", the user will select and enter via remote controller 120, the number "6" from the first set of association 502 because it appears directly above the number "6" in the second set, which corresponds to the second digit of his PIN.

[0036] FIG. 5C illustrates the third screen displayed to the user. As shown in FIG. 5C, the third screen contains substantially the same information as the previous screens, except that an asterisk now appears in both fields 506a and 506b, indicating that the second digit transmitted has also been received. In addition, the third screen's instructions are directed to requesting entry of the third digit of the user's PIN in accordance with the displayed association, Since the user's PIN is "7654", the user will select and enter the number "8" from the first set of the displayed association because it appears directly above the number "5" in the second set, which corresponds to the third digit of his PIN.

[0037] FIG. 5D illustrates the fourth screen displayed to the user. Asterisks now appear in fields 506a-c, indicating that the third digit transmitted has also been received. Also, the fourth screen's instructions are directed to requesting entry of the fourth digit of the user's PIN. The user will select the number "0" from the first set of the displayed association because it appears directly above the number "4" in the second set, which corresponds to the fourth and final digit of his PIN.

[0038] FIG. 5E illustrates the last screen displayed to the user. Asterisks now appear in all fields 506a-d, indicating that all four digits of the user's PIN have been received. The last screen's instructions are directed to requesting that the user stand by while the user's PIN is validated. As discussed above in connection with FIG. 3, if the decoded PIN is valid, the user is provided with access to the requested service/transaction. If, however, it is determined that the decoded PIN is not valid, then a screen indicating such may be displayed and, thereafter, the first screen of FIG. 5A may be re-displayed to request re-entry of an encoded PIN in accordance with a newly generated association 502 (i.e., the association is changed each time by terminal 200 as an added measure of security).

[0039] The many features and advantages of the present invention are apparent from the detailed specification, and thus, it is intended by the appended claims to cover all such features and advantages of the invention which fall within the true spirit and scope of the invention.

[0040] Furthermore, since numerous modifications and variations will readily occur to those skilled in the art, it is not desired that the present invention be limited to the exact construction and operation illustrated and described herein, and accordingly, all suitable modifications and equivalents which may be resorted to are intended to fall within the scope of the claims. For example, it is to be understood that the above-described hardware and functionality of electronic device 110 and terminal device 120 could be combined into a single device without departing from the spirit and scope of the present invention.

Claims

1. A method for enabling a user to transmit data in a secure manner over a wireless connection, comprising:

   displaying rules for encoding data;
   receiving encoded data over a wireless connection; and
   decoding the encoded data.

2. The method of claim 1, wherein the data comprises a personal identification number ("PIN").

3. The method of claim 2, wherein the data comprises payment information.

4. The method of claim 1, wherein the rules are automatically changed in a predetermined manner.

5. The method of claim 1, wherein the rules are displayed on a display of a device selected from the group consisting of a television and a personal computer.

6. The method of claim 5, wherein the encoded data is received from a remote control device.

7. The method of claim 6, wherein the remote control device is used to operate the device on whose display the rules are displayed.

8. The method of claim 1, wherein the wireless connection is an infrared or radio frequency wireless connection.

9. The method of claim 8, wherein the radio frequency wireless connection is a low power radio frequency ("LPRF") connection.

10. The method of claim 9, wherein the LPRF connec-

tion is a Bluetooth connection.

11. The method of claim 1, wherein the encoded data is decoded using the displayed rules.

12. The method of claim 2, further comprising:

validating the PIN; and
if the PIN is valid, permitting the user to engage in an activity.

13. The method of claim 12, wherein the step of validating comprises:

determining whether the PIN matches a PIN stored in a smart card.

14. A method for enabling a user to transmit data in a secure manner over a wireless connection, comprising:

viewing rules for encoding data for secure transmission over the wireless connection;
encoding the data in accordance with the rules; and
transmitting the encoded data over the wireless connection.

15. The method of claim 14, wherein the data comprises a personal identification number ("PIN").

16. The method of claim 14, wherein the data comprises payment information.

17. The method of claim 14, wherein the rules are automatically changed in a predetermined manner.

18. The method of claim 14, wherein the encoded data includes digits selected from the group consisting of numeric, alphabetic and symbolic characters.

19. The method of claim 14, wherein the rules are viewed on a display of a television, personal computer or a secured user interface.

20. The method of claim 14, wherein the wireless connection is an infrared or radio frequency wireless connection.

21. The method of claim 20, wherein the radio frequency wireless connection is a low power radio frequency ("LPRF") connection.

22. The method of claim 21, wherein the LPRF connection is a Bluetooth connection.

23. The method of claim 15, further comprising:

if the PIN is valid, engaging in an activity otherwise not permitted without a valid PIN.

24. The method of claim 23, wherein the step of validating includes determining whether the PIN matches a PIN stored in a smart card.

25. A system for enabling a user of a remote control device to transmit data in a secure manner over a wireless connection, comprising:

a memory device storing a program; and
a processor in communication with the memory device, the processor operative with the program to:

display rules for encoding data;
receive encoded data over a wireless connection; and
decode the encoded data.

26. The system of claim 25, wherein the data comprises a PIN.

27. The system of claim 25, wherein the encoded data is received from a remote controller.

28. The method of claim 25, wherein the processor is further operative with the program to validate the decoded data.

29. The system of claim 25, wherein the memory device and processor reside within a smart card.

30. A system for enabling a user of a remote control device to transmit data in a secure manner over a wireless connection, comprising:

a memory device storing a program; and
a processor in communication with the memory device, the processor operative with the program to:

display rules for encoding a PIN;
receive an encoded PIN over a wireless connection from a remote controller;
decode the encoded PIN;
validate the PIN; and
if said PIN is valid, permit access to an activity.

31. The system of claim 30, wherein the memory device and processor reside within a smart card.

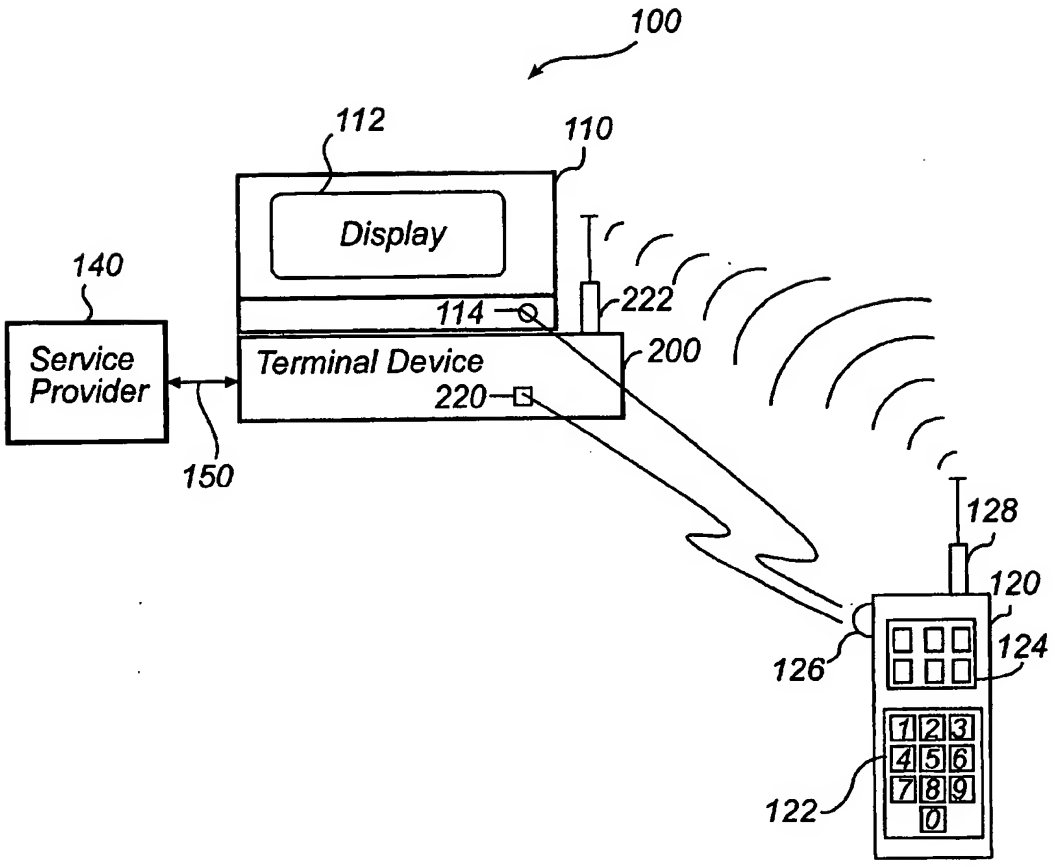
100
112
110
Display
140
222
114
Service Provider
Terminal Device
200
220
150
128
120
126
124
1 2 3
4 5 6
7 8 9
0
122

Fig. 1

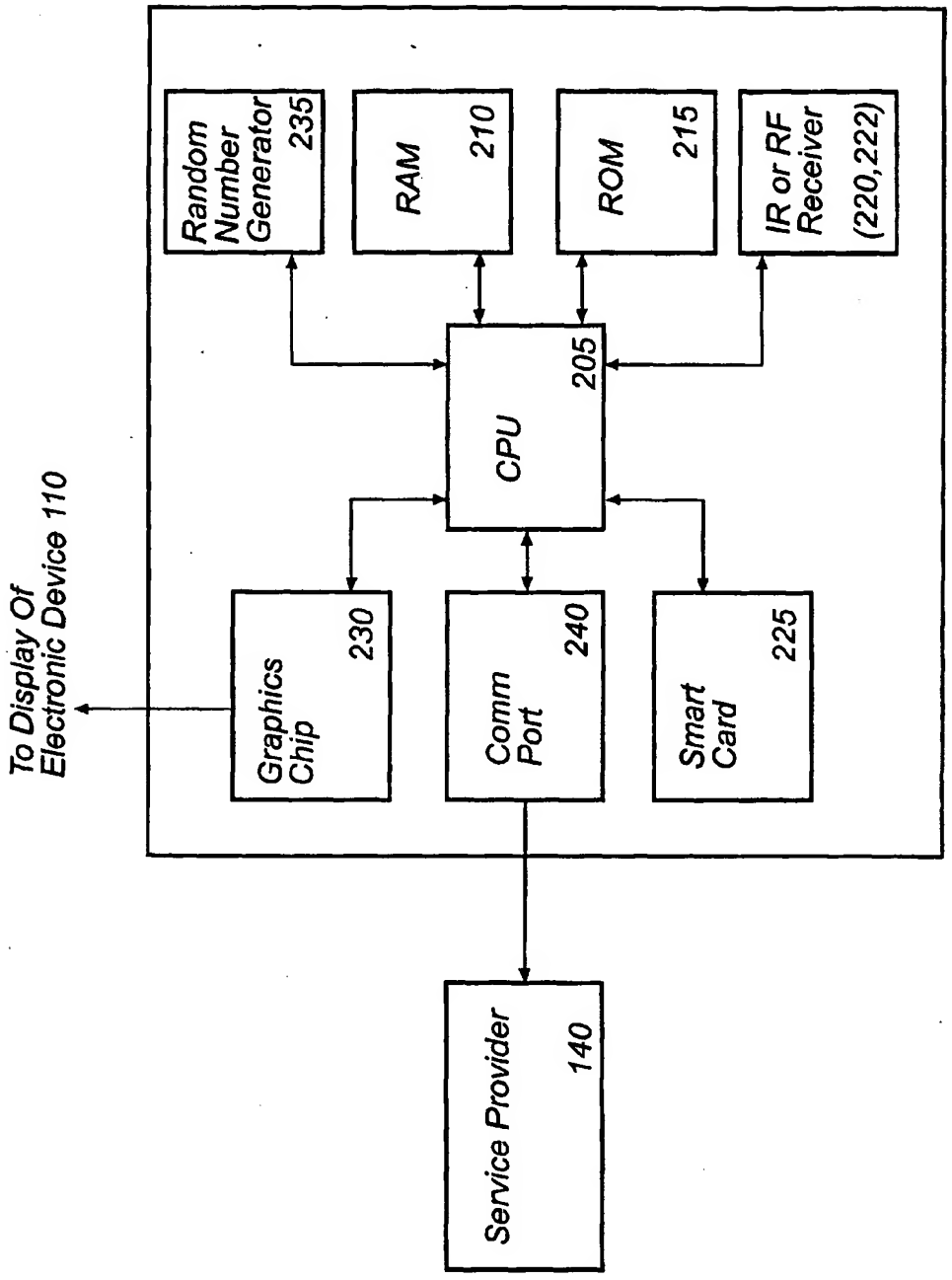
Random Number Generator 235
RAM 210
ROM 215
IR or RF Receiver (220,222)
CPU 205
Graphics Chip 230
Comm Port 240
Smart Card 225
To Display Of Electronic Device 110
Service Provider 140

Fig. 2

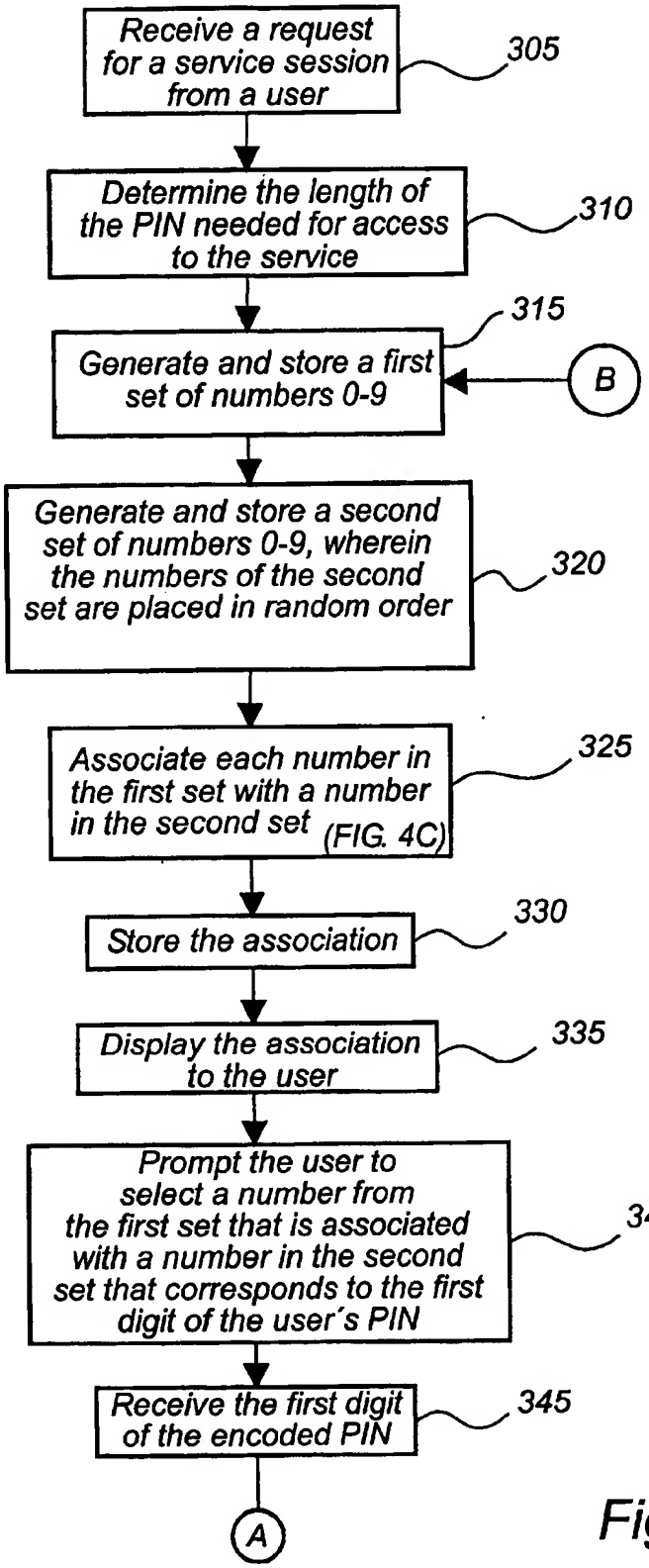
Receive a request for a service session from a user
305
Determine the length of the PIN needed for access to the service
310
315
Generate and store a first set of numbers 0-9
B
Generate and store a second set of numbers 0-9, wherein the numbers of the second set are placed in random order
320
Associate each number in the first set with a number in the second set (FIG. 4C)
325
Store the association
330
Display the association to the user
335
Prompt the user to select a number from the first set that is associated with a number in the second set that corresponds to the first digit of the user's PIN
340
Receive the first digit of the encoded PIN
345
A

Fig. 3

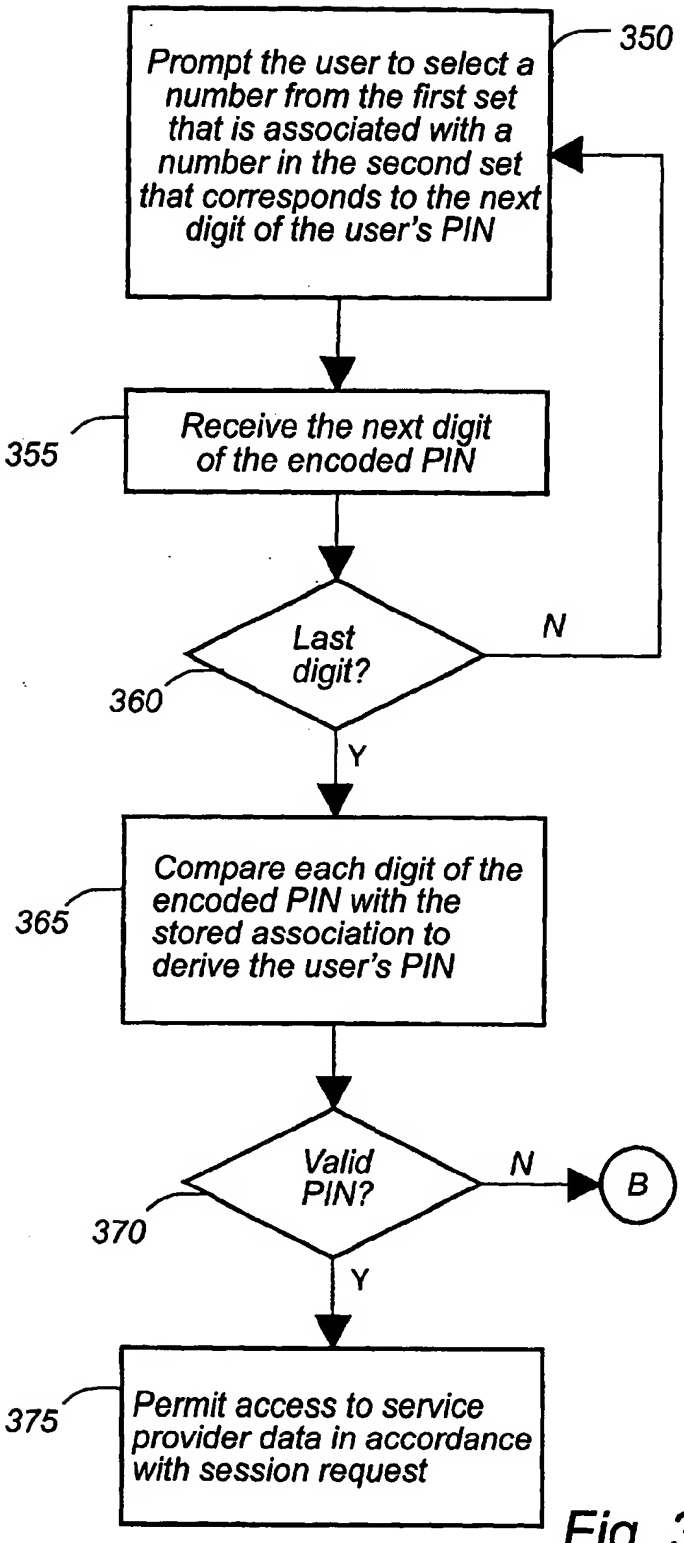
Prompt the user to select a number from the first set that is associated with a number in the second set that corresponds to the next digit of the user's PIN
350
Receive the next digit of the encoded PIN
355
Last digit?
360
N
Y
Compare each digit of the encoded PIN with the stored association to derive the user's PIN
365
Valid PIN?
370
N
B
Y
Permit access to service provider data in accordance with session request
375

Fig. 3 (Cont.)

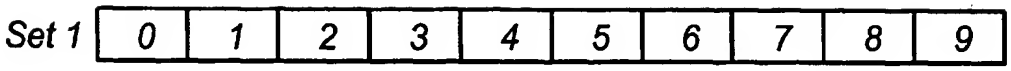

FIG. 4A

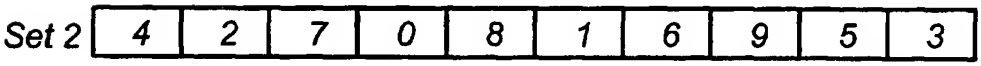

FIG. 4B

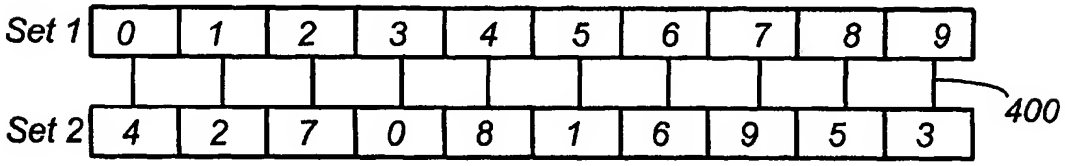

FIG. 4C

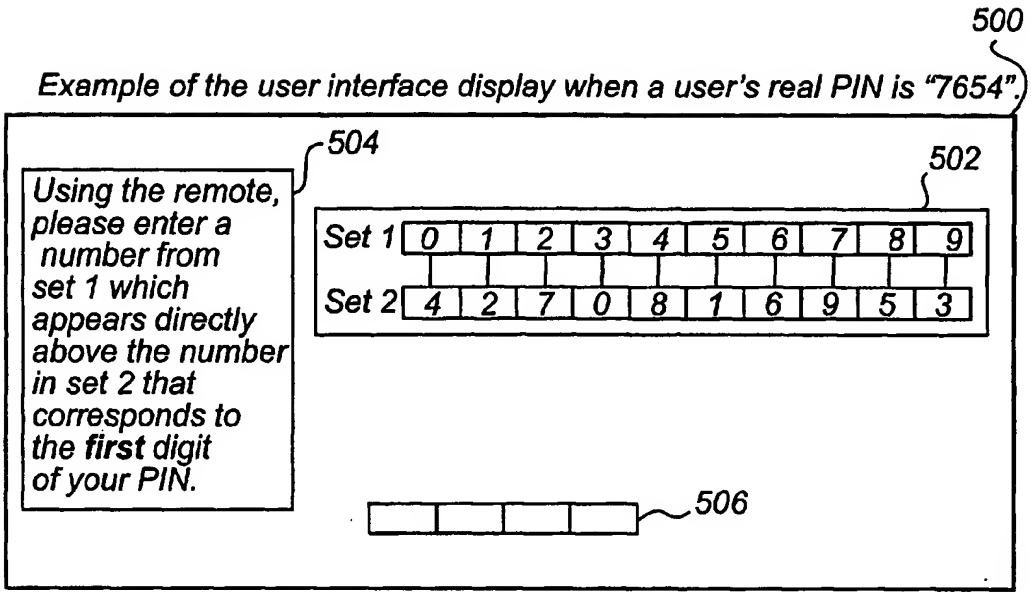
500
Example of the user interface display when a user's real PIN is "7654".
504
Using the remote, please enter a number from set 1 which appears directly above the number in set 2 that corresponds to the first digit of your PIN.
502
Set 1 0 1 2 3 4 5 6 7 8 9
Set 2 4 2 7 0 8 1 6 9 5 3
506

Fig. 5A

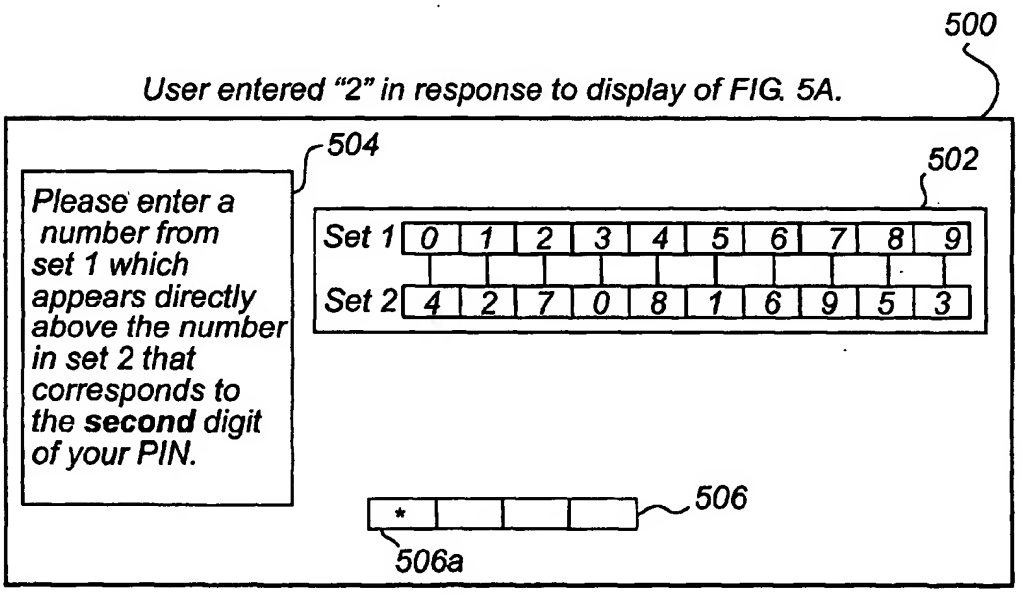
500
User entered "2" in response to display of FIG. 5A.
504
Please enter a number from set 1 which appears directly above the number in set 2 that corresponds to the second digit of your PIN.
502
Set 1 0 1 2 3 4 5 6 7 8 9
Set 2 4 2 7 0 8 1 6 9 5 3
*
506
506a

Fig. 5B

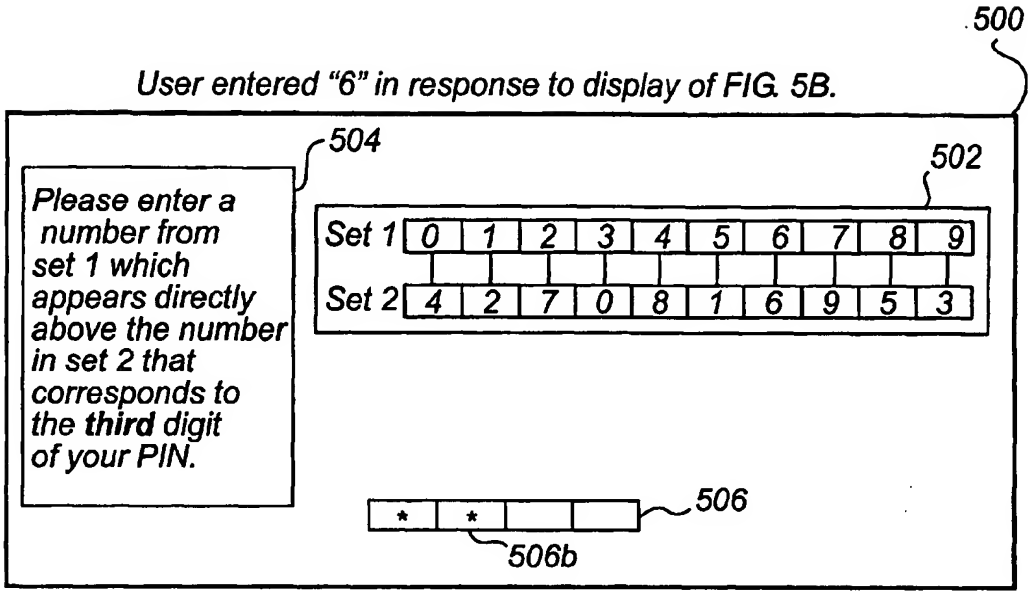
500
User entered "6" in response to display of FIG. 5B.
504
502
Please enter a number from set 1 which appears directly above the number in set 2 that corresponds to the third digit of your PIN.
Set 1 0 1 2 3 4 5 6 7 8 9
Set 2 4 2 7 0 8 1 6 9 5 3
506
506b

Fig. 5C

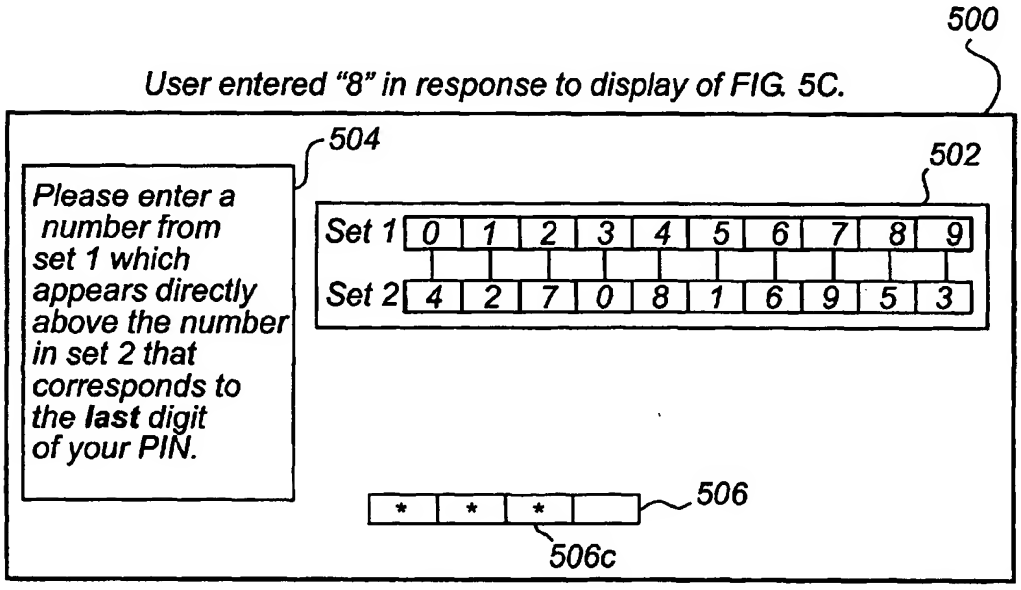
500
User entered "8" in response to display of FIG. 5C.
504
502
Please enter a number from set 1 which appears directly above the number in set 2 that corresponds to the last digit of your PIN.
Set 1 0 1 2 3 4 5 6 7 8 9
Set 2 4 2 7 0 8 1 6 9 5 3
506
506c

Fig. 5D

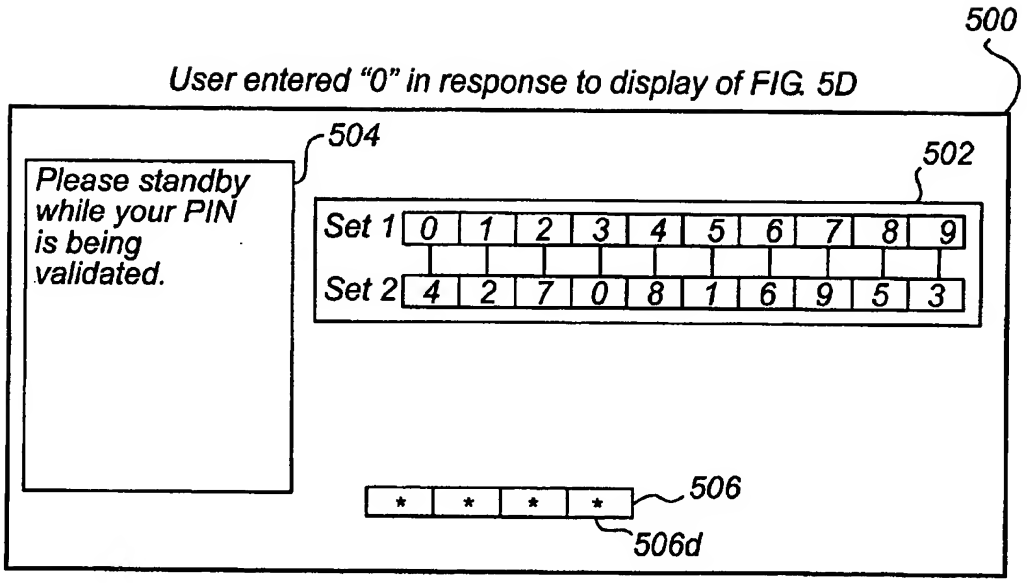
500
User entered "0" in response to display of FIG. 5D
504
502
Please standby while your PIN is being validated.
Set 1 0 1 2 3 4 5 6 7 8 9
Set 2 4 2 7 0 8 1 6 9 5 3
* * * *
506
506d

Fig. 5E

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 01 3660

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 5 177 789 A (COVERT JOHN R) 5 January 1993 (1993-01-05) * abstract * * column 2, line 15 - line 43 * * figures 1,4 *	1-30	H04L29/06 G07F7/10
Y	WO 98 43427 A (BASTIEN JEAN PAUL ;DECLERCK CHRISTOPHE (FR); CANAL PLUS SA (FR); B) 1 October 1998 (1998-10-01) * abstract * * page 5, line 18 - page 7, line 32 * * page 24, line 16 - page 27, line 7 * * figure 12 *	1-30	
A	WO 98 00968 A (FCA CORP DOING BUSINESS AS FOR) 8 January 1998 (1998-01-08) * abstract * * page 2, line 15 - page 3, line 19 * * page 16, line 15 - page 17, line 9 * * page 8, line 11 - line 16 * * figures 6A-6H,10 *	1-31	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
A	EP 0 690 399 A (TANDEM COMPUTERS INC) 3 January 1996 (1996-01-03) * abstract * * column 1, line 54 - column 4, line 36 * * column 9, line 22 - line 35 *	1-31	H04L G07F H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	24 October 2002	Bertolissi, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 01 3660

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

24-10-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5177789 A	05-01-1993	NONE	
WO 9843427 A	01-10-1998	WO 9843427 A1	01-10-1998
		AT 225108 T	15-10-2002
		AU 744977 B2	07-03-2002
		AU 2771097 A	20-10-1998
		BR 9714627 A	06-08-2002
		EP 0968608 A1	05-01-2000
		HU 0002384 A2	28-10-2000
		JP 2001517409 T	02-10-2001
		NO 994541 A	22-11-1999
		PL 335584 A1	08-05-2000
		AT 226003 T	15-10-2002
		AU 742213 B2	20-12-2001
		AU 746305 B2	18-04-2002
		AU 745783 B2	28-03-2002
		AU 741114 B2	22-11-2001
		AU 746178 B2	18-04-2002
		AU 744517 B2	28-02-2002
		AU 2770697 A	20-10-1998
		AU 742956 B2	17-01-2002
		AU 742067 B2	13-12-2001
		AU 740740 B2	15-11-2001
		AU 739663 B2	18-10-2001
		AU 745672 B2	28-03-2002
		AU 740887 B2	15-11-2001
		AU 7038198 A	20-10-1998
		AU 740632 B2	08-11-2001
		AU 740224 B2	01-11-2001
		BR 9714590 A	17-09-2002
		BR 9714591 A	17-09-2002
		BR 9714598 A	06-08-2002
		BR 9714599 A	10-09-2002
		BR 9714600 A	10-09-2002
		BR 9714601 A	10-09-2002
		BR 9714602 A	17-09-2002
		BR 9714603 A	16-05-2000
		BR 9714604 A	06-08-2002
		BR 9714649 A	06-08-2002
		BR 9808283 A	16-05-2000
		BR 9808288 A	16-05-2000
		CN 1254472 A	24-05-2000
		CN 1260056 A	12-07-2000
		CN 1254477 A	24-05-2000
		CN 1254478 A	24-05-2000
		CN 1254469 A	24-05-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 01 3660

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

24-10-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9843427 A		CN 1254423 A	24-05-2000
		CN 1262754 A	09-08-2000
		CN 1254473 A	24-05-2000
		CN 1254422 A	24-05-2000
WO 9800968 A	08-01-1998	US 5973756 A	26-10-1999
		AU 3957397 A	21-01-1998
		EP 0906691 A1	07-04-1999
		WO 9800968 A1	08-01-1998
		US 6275991 B1	14-08-2001
EP 0690399 A	03-01-1996	CA 2153006 A1	31-12-1995
		CN 1118482 A	13-03-1996
		EP 0690399 A2	03-01-1996
		JP 8063532 A	08-03-1996
		US 5999624 A	07-12-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82